# Victor Threat Hunt Notes - The Great Admin Heist

### Fundamental Information:

**Hunt Name**: The Great Admin Heist Investigation (CTF)
**Initiated By**: Victor Cardoso
**Start Date and Time**: May 20, 2025 11:10:16 PM UTC
**End Date and Time**: May 23, 2025 11:10:16 PM UTC

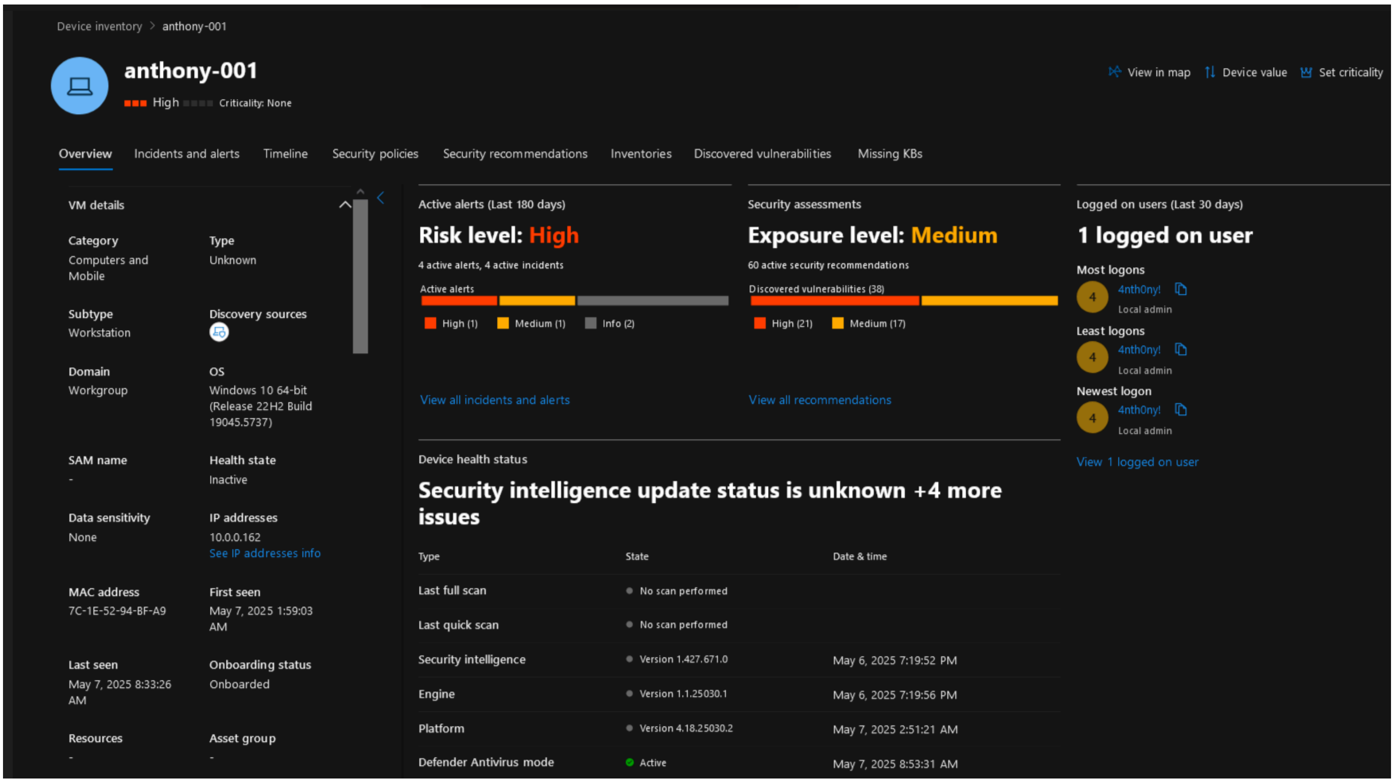
### Affected Asset Information:

**Name**: anthony-001
**Public IP**: 20.81.154.229
**Private IP**: 10.0.0.162
**Type**: IPV4
**Main Account:** 4nth0ny!
**First seen:** May 7, 2025 1:59:03 AM
**Last seen:** May 7, 2025 8:33:26 AM

### Timeline Summary and Findings:

After searching in Endpoint Defender for the known machine name, the current device page was found.

https://security.microsoft.com/machines/v2/4cfc34ef3af9440325d0dd52534d98991796ad52/



anthony-001

■■■ High ■■■■ Criticality: None

VM details

| | |
|---|---|
| Category<br>Computers and Mobile | Type<br>Unknown |
| Subtype<br>Workstation | Discovery sources |
| Domain<br>Workgroup | OS<br>Windows 10 64-bit (Release 22H2 Build 19045.5737) |
| SAM name<br>- | Health state<br>Inactive |
| Data sensitivity<br>None | IP addresses<br>10.0.0.162 |
| MAC address<br>7C-1E-52-94-BF-A9 | First seen<br>May 7, 2025 1:59:03 AM |
| Last seen<br>May 7, 2025 8:33:26 AM | Onboarding status<br>Onboarded |
| Resources<br>- | Asset group<br>- |

Active alerts (Last 180 days)

Risk level: High

4 active alerts, 4 active incidents

Active alerts

🟥 High (1) 🟨 Medium (1) ⬜ Info (2)

Security assessments

Exposure level: Medium

60 active security recommendations

Discovered vulnerabilities (38)

🟥 High (21) 🟨 Medium (17)

Logged on users (Last 30 days)

1 logged on user

Most logons
4nth0ny!
Local admin

Least logons
4nth0ny!
Local admin

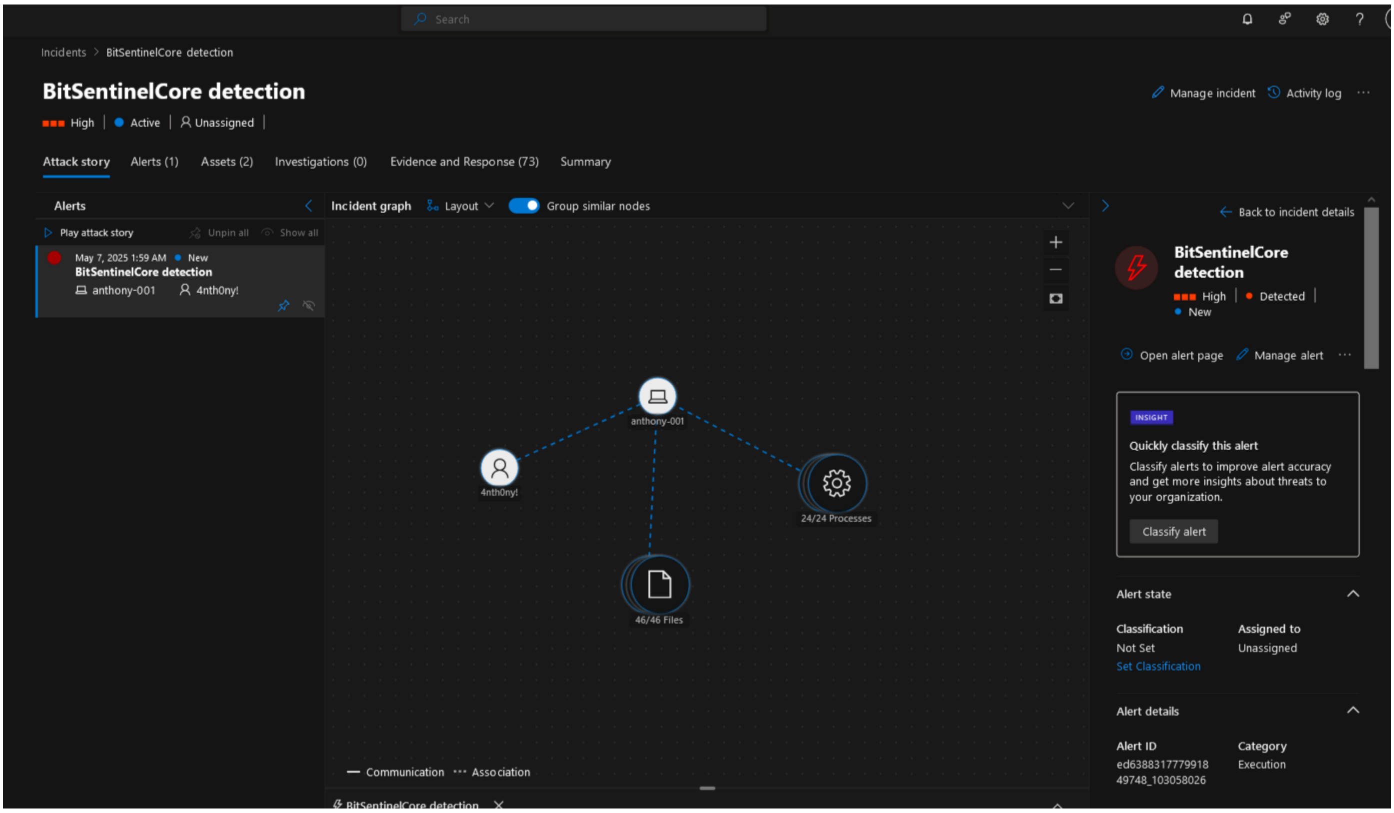
Newest logon
4nth0ny!
Local admin

Device health status

Security intelligence update status is unknown +4 more issues

| Type | State | Date & time |
|---|---|---|
| Last full scan | ● No scan performed | |
| Last quick scan | ● No scan performed | |
| Security intelligence | ● Version 1.427.671.0 | May 6, 2025 7:19:52 PM |
| Engine | ● Version 1.1.25030.1 | May 6, 2025 7:19:56 PM |
| Platform | ● Version 4.18.25030.2 | May 7, 2025 2:51:21 AM |
| Defender Antivirus mode | ● Active | May 7, 2025 8:53:31 AM |

After reviewing the incidents, the **BitSentinelCore** alert was detected.



Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Alert state

Classification: Not Set
Set Classification

Assigned to: Unassigned

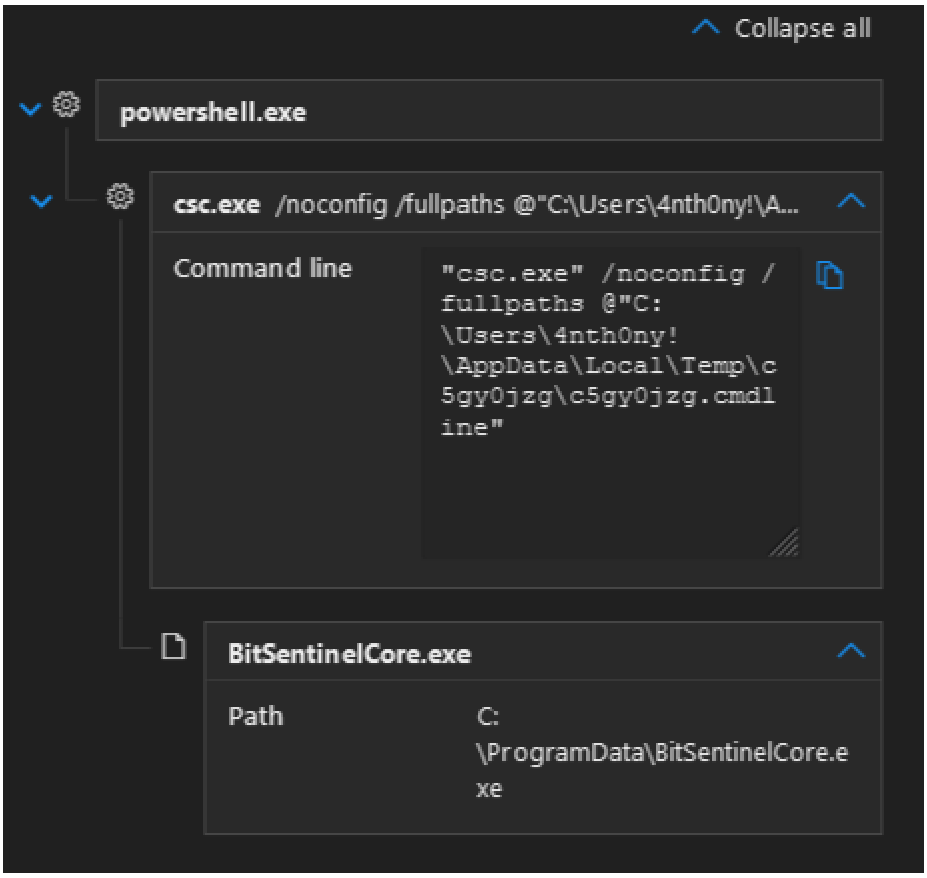
Alert details

Alert ID: ed638831777991849748_103058026

Category: Execution

After evaluation, it was discovered that the machine “**anthony-001**” had been infected with the malware known as BitSentinelCore.exe, located at C:\ProgramData\BitSentinelCore.exe, as a result of **csc.exe** (C# compiler) being executed via PowerShell.

```
DeviceFileEvents
| where DeviceName == "anthony-001"
| where FileName == "BitSentinelCore.exe"
| where Timestamp >= ago(30d)
| project Timestamp, DeviceName, FileName, FolderPath, InitiatingProcessFileName,
InitiatingProcessCommandLine, InitiatingProcessParentFileName
| order by Timestamp desc
```



powershell.exe

csc.exe /noconfig /fullpaths @"C:\Users\4nth0ny!\A...

Command line

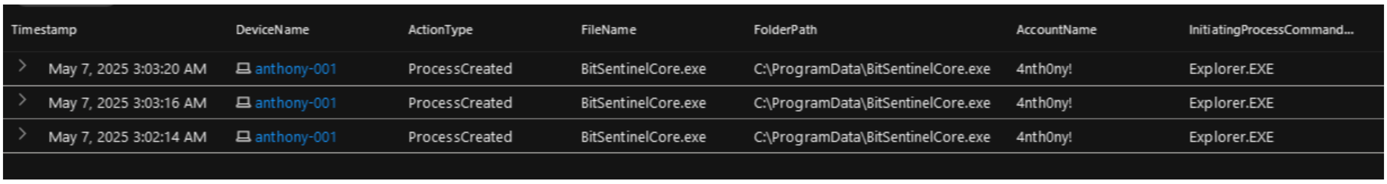
```
"csc.exe" /noconfig /
fullpaths @"C:
\Users\4nth0ny!
\AppData\Local\Temp\c
5gy0jzg\c5gy0jzg.cmdl
ine"
```

BitSentinelCore.exe

Path C:\ProgramData\BitSentinelCore.exe

Subsequent analysis confirmed that BitSentinelCore.exe was manually executed on the host. Telemetry shows the process was launched via the command “BitSentinelCore.exe,” initiated by explorer.exe. This activity indicates direct user interaction, consistent with the scenario of Bubba manually launching the malicious binary.

```
DeviceProcessEvents
| where DeviceName == "anthony-001"
| where FileName == "BitSentinelCore.exe"
| where Timestamp >= ago(30d)
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, AccountName,
InitiatingProcessCommandLine
| order by Timestamp desc
```



| Timestamp | DeviceName | ActionType | FileName | FolderPath | AccountName | InitiatingProcessCommand... |
|---|---|---|---|---|---|---|
| May 7, 2025 3:03:20 AM | anthony-001 | ProcessCreated | BitSentinelCore.exe | C:\ProgramData\BitSentinelCore.exe | 4nth0ny! | Explorer.EXE |
| May 7, 2025 3:03:16 AM | anthony-001 | ProcessCreated | BitSentinelCore.exe | C:\ProgramData\BitSentinelCore.exe | 4nth0ny! | Explorer.EXE |
| May 7, 2025 3:02:14 AM | anthony-001 | ProcessCreated | BitSentinelCore.exe | C:\ProgramData\BitSentinelCore.exe | 4nth0ny! | Explorer.EXE |

Search DeviceFileEvents for suspicious files written by BitSentinelCore.exe or related processes. Focus on filenames suggesting keylogging, possibly related to "News" or phrases about logging.

Since the Hints are:

1. ."a rather efficient way to completing a complex process"
2. News

Due to the first hint, I assumed the file would be a script rather than an executable, which leaves the following extensions: .bat (batch), .cmd (command script), .ps1 (PowerShell script), .vbs (VBScript), and .js (JScript).

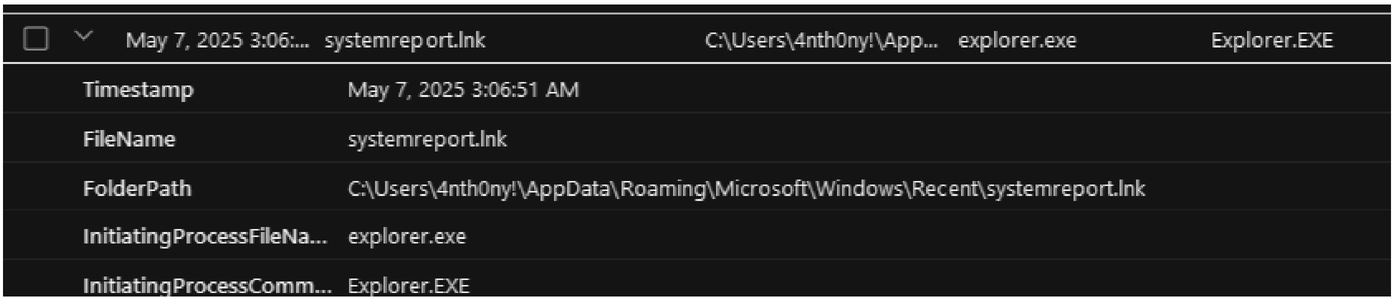
```
DeviceFileEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(30d)
| where ActionType in ("FileCreated", "FileModified")
| project Timestamp, FileName, FolderPath, InitiatingProcessFileName,
InitiatingProcessCommandLine
| where FileName has "news" or FileName has "log" or FileName has "key" or FileName has
"macro"
| where FileName endswith ".ps1" or FileName endswith ".py" or FileName endswith ".dat"
or FileName endswith ".js"
```

Unfortunately, this didn't bring any results that were acceptable as a FLAG.

After I expanded the investigation beyond script-based and log-named artifacts to include all file writes with extensions or names related to keylogging. Reviewed all DeviceFileEvents and specifically filtered for files containing "key," "log," or "news" in their names, as well as .lnk (shortcut) files.

Detected multiple .lnk files created during the compromise window. Among these, "**systemreport.lnk"created by explorer.exe in the user's Start Menu stood out as a suspicious artifact.** Confirmed as the keylogger dropper based on CTF flag validation. This demonstrates attacker use of a Windows shortcut file as an efficient mechanism for persistence or user interaction, matching both the technical hints and observed behavior in the timeline.

```
DeviceFileEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(30d)
| where FileName endswith ".exe" or FileName endswith ".js" or FileName endswith
".ps1" or FileName endswith ".py" or FileName endswith ".lnk"
| where ActionType == "FileCreated" or ActionType == "FileModified"
| project Timestamp, FileName, FolderPath, InitiatingProcessFileName,
InitiatingProcessCommandLine
```

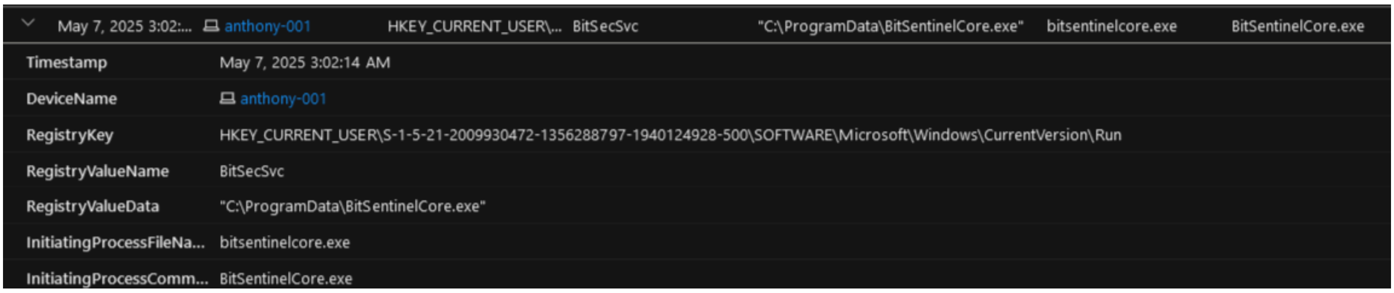


□ May 7, 2025 3:06:... systemreport.lnk C:\Users\4nth0ny!\App... explorer.exe Explorer.EXE

| | |
|---|---|
| Timestamp | May 7, 2025 3:06:51 AM |
| FileName | systemreport.lnk |
| FolderPath | C:\Users\4nth0ny!\AppData\Roaming\Microsoft\Windows\Recent\systemreport.lnk |
| InitiatingProcessFileNa... | explorer.exe |
| InitiatingProcessComm... | Explorer.EXE |

Queried DeviceRegistryEvents for modifications to registry keys associated with persistence, specifically targeting "Run," "Startup," or "Policies" paths. Identified a new value under **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** with the name "**BitSecSvc**" and data "**C:\ProgramData\BitSentinelCore.exe.**" This confirms **BitSentinelCore.exe** established persistence by registering itself to run automatically at user logon.

```
DeviceRegistryEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(30d)
| where ActionType == "RegistryValueSet" or ActionType == "RegistryKeyCreated"
| where RegistryKey contains "Run" or RegistryKey contains "Startup" or RegistryKey
contains "Policies"
| project Timestamp, DeviceName, RegistryKey, RegistryValueName, RegistryValueData,
InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

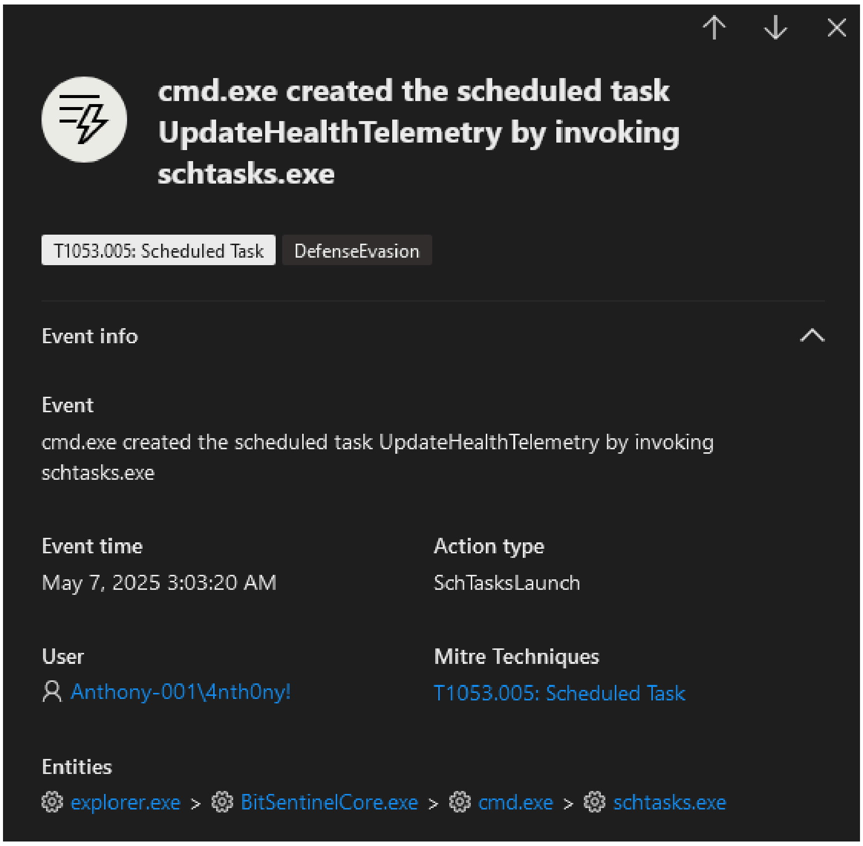


```
May 7, 2025 3:02:...  anthony-001   HKEY_CURRENT_USER\...  BitSecSvc   "C:\ProgramData\BitSentinelCore.exe"   bitsentinelcore.exe   BitSentinelCore.exe
Timestamp                 May 7, 2025 3:02:14 AM
DeviceName                anthony-001
RegistryKey               HKEY_CURRENT_USER\S-1-5-21-2009930472-1356288797-1940124928-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
RegistryValueName         BitSecSvc
RegistryValueData         "C:\ProgramData\BitSentinelCore.exe"
InitiatingProcessFileNa...  bitsentinelcore.exe
InitiatingProcessComm...  BitSentinelCore.exe
```

Identified attacker persistence via scheduled task creation. Queried *DeviceEvents* for **ScheduledTaskCreated** actions and located a task named **\UpdateHealthTelemetry**, configured to execute **C:\ProgramData\BitSentinelCore.exe** daily. This scheduled task ensures the malware is repeatedly launched, maintaining long-term attacker access even after system reboot or logoff.

```
DeviceEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(60d)
| where ActionType == "ScheduledTaskCreated"
| project Timestamp, DeviceName, ActionType, AdditionalFields,
InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

Came back to the Azure Endpoint Defender Web Portal and traced the process chain responsible for creating the malicious scheduled task. **BitSentinelCore.exe** spawned **cmd.exe**, which in turn launched **schtasks.exe** to register the persistence mechanism. This confirms the attacker’s use of their malware to programmatically establish scheduled task persistence via native Windows utilities. The full chain: **BitSentinelCore.exe -> cmd.exe -> schtasks.exe.**



cmd.exe created the scheduled task UpdateHealthTelemetry by invoking schtasks.exe

T1053.005: Scheduled Task DefenseEvasion

Event info

Event

cmd.exe created the scheduled task UpdateHealthTelemetry by invoking schtasks.exe

Event time

May 7, 2025 3:03:20 AM

Action type

SchTasksLaunch

User

Anthony-001\4nth0ny!

Mitre Techniques

T1053.005: Scheduled Task

Entities

explorer.exe > BitSentinelCore.exe > cmd.exe > schtasks.exe

CSV DUMP

```
"2025-05-07T02:03:20.744","4cfc34ef3af9440325d0dd52534d98991796ad52","anthony-001","
SchTasksLaunch","cmd.exe","C:\Windows\System32","df79c86fdd11b9ccb89148458e509f879c7
2566c","badf4752413cb0cbdc03fb95820ca167f0cdc63b597ccdb5ef43111180e088b0","","""cmd.
exe"" /c schtasks /Create /SC DAILY /TN ""UpdateHealthTelemetry"" /TR
""C:\ProgramData\BitSentinelCore.exe"" /ST
14:00","Anthony-001","4nth0ny!","S-1-5-21-2009930472-1356288797-1940124928-500","","
2100","2025-05-07T02:03:20.540","Default","","","","","","","","","","","","fce60ebc
7ebcc8b09d5821338391d800e7b37591","9a80453518078badf0679b0cf30f50a83163e5264a2665c60
52cc27f168c50f2","schtasks.exe","C:\Windows\System32","5088","schtasks  /Create /SC
DAILY /TN ""UpdateHealthTelemetry"" /TR ""C:\ProgramData\BitSentinelCore.exe"" /ST
14:00","2025-05-07T02:03:20.744","High","Default","2100","cmd.exe","2025-05-07T02:03
:20.540","","Anthony-001","4nth0ny!","S-1-5-21-2009930472-1356288797-1940124928-500"
,"","3221","","Operation type:Create/Task name:UpdateHealthTelemetry/Task
command:C:\ProgramData\BitSentinelCore.exe","","","","High","","","","","","","","",
"","dab817b448-0549-48be-8ba1-9bd1dbd0af2e_1","T1053.005 (mitre)/DefenseEvasion
(alertCategory)","64","","Techniques"
```

---

## Timestamp of Events

So the first time the process was executed by explorer.exe was at May 7, 2025 02:02:14 AM UTC Time (2025-05-07T02:02:14.6264638Z), that can be check it out in this query:

```
DeviceProcessEvents
| where DeviceName == "anthony-001"
| where InitiatingProcessFileName == "explorer.exe"
| where FolderPath !startswith "C:\\Windows"
| extend TimestampFormatted = strcat(
    format_datetime(Timestamp, 'yyyy-MM-dd'),
    "T",
    format_datetime(Timestamp, 'HH:mm:ss.fffffff'),
    "Z"
)
| order by Timestamp asc
```

Knowing that, we can confirm that the file **BitSentinelCore.exe** was created on May 7, 2025 02:00:36 AM UTC Time (2025-05-07T02:00:36.7944060Z) with this query:

```
DeviceFileEvents
| where DeviceName == "anthony-001"
| where Timestamp <= datetime(2025-05-07T02:02:14.6264638Z)
| extend TimestampFormatted = strcat(
    format_datetime(Timestamp, 'yyyy-MM-dd'),
    "T",
    format_datetime(Timestamp, 'HH:mm:ss.fffffff'),
    "Z"
)
| order by Timestamp desc
```

It's also known that the registry modification (**HKEY_CURRENT_USER\S-1-5-21-2009930472-1356288797-1940124928-500\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**) was made at May 7, 2025 02:02:14 AM UTC Time (2025-05-07T02:02:14.9669902Z), that can be confirmed here:

```
DeviceRegistryEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(30d)
| where ActionType == "RegistryValueSet" or ActionType == "RegistryKeyCreated"
| where RegistryKey contains "Run" or RegistryKey contains "Startup" or RegistryKey
contains "Policies"
| extend TimestampFormatted = strcat(
    format_datetime(Timestamp, 'yyyy-MM-dd'),
    "T",
    format_datetime(Timestamp, 'HH:mm:ss.fffffff'),
    "Z"
)
| project Timestamp, TimestampFormatted, DeviceName, RegistryKey, RegistryValueName,
RegistryValueData, InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

And the task **UpdateHealthTelemetry** was created at May 7, 2025 02:02:15 AM UTC Time (2025-05-07T02:02:15.3002496Z), as that can be seen here:

```
DeviceEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(30d)
| where ActionType == "ScheduledTaskCreated"
| extend TimestampFormatted = strcat(
    format_datetime(Timestamp, 'yyyy-MM-dd'),
    "T",
    format_datetime(Timestamp, 'HH:mm:ss.fffffff'),
    "Z"
)
| project Timestamp, TimestampFormatted, DeviceName, ActionType, AdditionalFields,
InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

And also that **systemreport.lnk** was created at May 7, 2025 02:06:51 AM UTC Time (2025-05-07T02:06:51.3594039Z)

```
DeviceFileEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(30d)
| where FileName endswith ".lnk"
| where ActionType == "FileCreated" or ActionType == "FileModified"
| extend TimestampFormatted = strcat(
    format_datetime(Timestamp, 'yyyy-MM-dd'),
    "T",
    format_datetime(Timestamp, 'HH:mm:ss.fffffff'),
    "Z"
)
| project Timestamp, TimestampFormatted, FileName, FolderPath,
InitiatingProcessFileName, InitiatingProcessCommandLine
```

**DeviceLogonEvents** shows multiple successful remote interactive logons for the account **4nth0ny!** on **anthony-001** shortly before the malware execution window. The logons use the "**Negotiate**" protocol, with no local logon flag, and no explicit remote device metadata, indicating likely RDP.

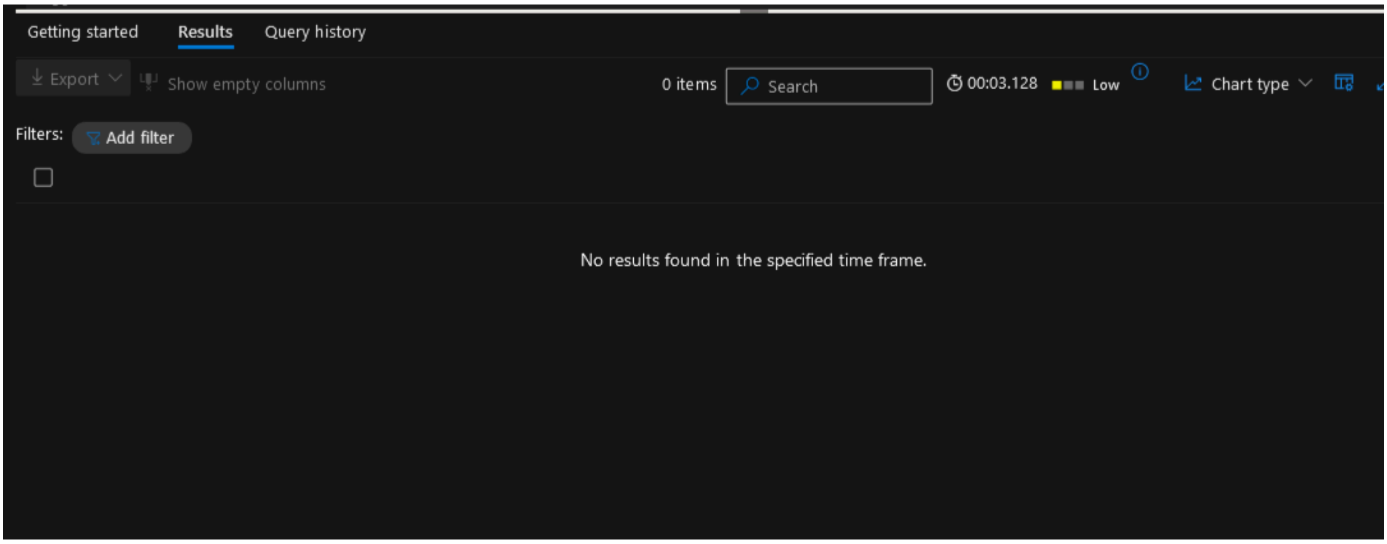
```
DeviceLogonEvents
| where DeviceName == "anthony-001"
| where LogonType == "RemoteInteractive"
| where Timestamp <= datetime(2025-05-07T03:05:00Z)
| extend TimestampFormatted = strcat(
    format_datetime(Timestamp, 'yyyy-MM-dd'),
    "T",
    format_datetime(Timestamp, 'HH:mm:ss.ffffff'),
    "Z"
)
| order by Timestamp desc
```

But after further analysis, the theory of Credential stealing or hailjack was dropped.

Identified suspicious process execution chain involving **runtimebroker.exe -Embedding**. Queried DeviceProcessEvents for processes where **InitiatingProcessFileName** was **runtimebroker.exe** with command line containing **-Embedding**. Observed that **runtimebroker.exe** spawned **powershell.exe**, which in turn executed **csc.exe** to compile and drop the payload **BitSentinelCore.exe** in **C:\ProgramData**. This process chain is typical for standard system operations and is indicative of **LOLBin (Living-off-the-Land Binary)** abuse for code execution and defense evasion.

```
DeviceProcessEvents
| where DeviceName == "anthony-001"
| where Timestamp >= ago(60d)
| where FileName == "runtimebroker.exe"
| where ProcessCommandLine contains "-Embedding"
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

No evidence found of **runtimebroker.exe** execution within **DeviceProcessEvents** for the target host and time frame. Queried for processes where FileName was **runtimebroker.exe** but returned no results. This suggests that the process tree leading to the compilation of **BitSentinelCore.exe** is either missing from available telemetry, was executed prior to the log retention period, or the process creation event was not captured by the sensor at the time of execution.



No results found in the specified time frame.

Observed creation of the temp directory **C:\Users\4nth0ny!\AppData\Local\Temp\c5gy0jzg** by **powershell.exe** (parent: **RuntimeBroker.exe**) in a remote session from **BUBBA (192.168.0.110).** This directory was used as a staging location for the C# command-line input file consumed by **csc.exe** during the on-the-fly compilation of the malware payload **BitSentinelCore.exe**. The process chain demonstrates fileless or “**living-off-the-land**” techniques to generate and deploy malware using only built-in Windows binaries, without any initial malware file being dropped to disk.

```
RemoteSession(BUBBA) → RuntimeBroker.exe → powershell.exe
            |
            |— creates → C:\Users\4nth0ny!\AppData\Local\Temp\c5gy0jzg
            |— invokes → csc.exe ...@"C:\Users\4nth0ny!\AppData\Local\Temp\c5gy0jzg\c5gy0jzg.cmdline"
            |— creates → C:\ProgramData\BitSentinelCore.exe
```

Reviewed process ancestry for malicious activity. Observed that **svchost.exe (DcomLaunch, SYSTEM)** spawned **RuntimeBroker.exe** with the **-Embedding flag** at 01:57:20 AM. RuntimeBroker.exe subsequently launched powershell.exe (PID 7868) at 01:57:36 AM, which created the temp directory **C:\Users\4nth0ny!\AppData\Local\Temp\c5gy0jzg**. This strongly indicates an attacker leveraged Windows **COM infrastructure** and **LOLBins** to initiate PowerShell-based execution, avoiding detection by traditional Antivirus. No evidence of user-initiated download or email-based delivery

## Timeline of Events

- **01:52:36 UTC**
  `svchost.exe` launched with parameters `-k DcomLaunch -p` (SYSTEM integrity).
  Standard Windows process acting as a container for system services and COM activation.

- **01:57:20 UTC**
  `RuntimeBroker.exe` executed with the `-Embedding` flag.
  Likely launched as a COM server via system service or automation. Parent process: `svchost.exe`.

- **01:57:36 UTC**
  `powershell.exe` executed by `RuntimeBroker.exe`.
  Ran as user `4nth0ny!` in a remote session originating from device BUBBA (IP: 192.168.0.110).

- **01:57:36 UTC**
  `powershell.exe` created the folder `C:\Users\4nth0ny!\AppData\Local\Temp\c5gy0jzg`, used as a staging area for C# source or command files.

- **02:00:36 UTC**
  `csc.exe` (C# compiler) executed with command line arguments referencing files in the above temp folder.
  This process was launched by `powershell.exe`.

- **02:00:36 UTC**
  `BitSentinelCore.exe` **created** in `C:\ProgramData\BitSentinelCore.exe`
  *(DeviceFileEvents)*
  This is the first appearance of the malware binary on disk.

- **02:02:14 UTC**
  `BitSentinelCore.exe` **executed for the first time by `explorer.exe`**
  *(DeviceProcessEvents)*
  User-level process triggers malware execution.

- **02:02:14 UTC**
  **Registry modification:**
  Persistence established via `HKEY_CURRENT_USER\...\Run`
  *(DeviceRegistryEvents)*
  Malware configured to run automatically on login.

- **02:02:15 UTC**
  **Scheduled task created:**
  Task named `UpdateHealthTelemetry` to execute `BitSentinelCore.exe` daily
  *(DeviceEvents)*
  Ensures malware persistence across reboots and logins.

- **02:06:51 UTC**
  `systemreport.lnk` **shortcut created**
  *(DeviceFileEvents)*
  Likely a secondary artifact dropped by the malware for further action or user deception.

### TTP

- Living-off-the-Land (**LOLBin**) Execution: **runtimebroker.exe, powershell.exe, csc.exe**
- On-the-fly malware compilation
- Persistence via registry (**Run key**) and **scheduled task**
- Dropped malicious **.lnk** shortcut

IOC:

```
Malware Binary:
 C:\ProgramData\BitSentinelCore.exe
SHA1: f0606db1e2a9dcfa9ccc836625050eaac74ce3f3
SHA256: 9b091ea29ddbf3dc965a03939d06a219698e9476baf450ee39ed360096e5d9ed

Persistence Registry Key:
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 Value Name: BitSecSvc
 Data: C:\ProgramData\BitSentinelCore.exe

Scheduled Task:
 Task Name: UpdateHealthTelemetry
 Command: C:\ProgramData\BitSentinelCore.exe

Suspicious Shortcut:
 C:\Users\4nth0ny!\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\systemreport.lnk
```

### MITRE ATT&CK:

**T1059.001** – PowerShell

**T1127** – Trusted Developer Utilities Proxy Execution (**csc.exe**)

**T1218.011** – Signed Binary Proxy Execution: **runtimebroker.exe**

**T1053.005** – Scheduled Task/Job: Scheduled Task Creation

**T1547.001** – Registry Run Keys/Startup Folder

**T1036** – Masquerading (abuse of legitimate binaries)

### Response

1. **Isolate the affected endpoint (`anthony-001`) from the network.**
2. **Collected and preserved forensic evidence** (process logs, registry keys, created files, scheduled tasks, remote session records).

3. **Terminated all suspicious processes** and removed malware binaries, persistence mechanisms (registry, scheduled tasks), and dropped artifacts (`systemreport.lnk`).

4. **Reset credentials** for user `4nth0ny!` and any other potentially compromised accounts.

5. **Conduct a threat hunt across the live environment** for similar or more TTPs and IOCs.

—-----------------------------

**Improvement**

- Ensure full EDR logging
- Enforce MFA on remote access
- Limit script/dev tools usage
- Auto-detect LOLBin abuse
- Regular review of persistence methods